# Проектирование системы защищенного дистанционного управления

**Любименко Дмитрий Анатольевич**
Главный специалист службы информационных инфраструктурных систем АО «СО ЕЭС», г. Волгоград, Россия, lubimenko-d@bk.ru

АННОТАЦИЯ

**Введение**: интеграция в систему мониторинга, управления субъектами энергетики защищенного дистанционного управления (ЗДУ), реализованного с помощью системы биометрического распознавания команд (СБПК). **Цель исследования**: разработка и внедрение информационно-управляющей системы для контроля пользователей с доступом к отправке команд дистанционного управления (ДУ) от коммуникационного процессора на субъекты энергетики. **Результаты**: информационно-управляющая система позволяет формировать информационные сообщения диспетчерскому персоналу, выполнять переключения посредством дистанционного управления. Выполнены проектировка комплекса, испытания, ввод в промышленную эксплуатацию. Развернута группа горячего резервирования из двух серверов Vegman Yadro. В качестве хостовой операционной системы используется Astra Linux Special Edition. Промышленные сервера, сканеры биометрии, коммутаторы доступа расположены в защищенной подсети (выделена в отдельный сегмент). Защита данных, шифрование трафика выполнено с использованием отечественного межсетевого экрана нового поколения Usergate D200, работающего в режиме кластера (active-passive). Разработана система идентификации, аутентификации пользователей в системе. Проверена функциональность системы передачи команд дистанционного управления. Группа горячего резервирования предполагает возможность снижения надежности на 50% (допускается выход из строя одного из серверов). Основная задача, предполагающая внедрение системы дистанционного управления, выполнена на 100%. **Практическая значимость**: система защищенного дистанционного управления позволяет обеспечить контроль пользователей с правами на отправку команд дистанционного управления от коммуникационного процессора СК11.Proxy, разработанного АО «Монитор Электрик». Средством санкционирования для отправки команды является биометрический сканер отпечатка пальца. Транспорт данных реализован с использованием протокола МЭК 60870-5-104. Реализовано логирование всех событий в системе, возникающих в результате подтверждений полномочий пользователей. Сохраняются данные о выполнении, отмене,подтверждении команд.

КЛЮЧЕВЫЕ СЛОВА: управление субъектами энергетики; дистанционное управление; система; команда; защищенное дистанционное управление

**Введение**

Современные энергетические системы в связи с возрастающей сложностью управления, внедрением новых субъектов генерации и потребления, транспортировки требуют большей автоматизации для снижения нагрузки на персонал оперативно-диспетчерского управления. Инновационным направлением является дистанционное управление переключениями.

Проект защищенного дистанционного управления, задействованного в АО СО «ЕЭС», реализован с использованием самых современных проектов и протоколов. 90% оборудования и программного обеспечения, используемого при реализации проекта, разработано и произведено в РФ.

Проектируемая информационно-управляющая система относится к объектам защищенной критической инфраструктуры. ФСТЭК предъявляет особые требования к используемому оборудованию, программному обеспечению. Готовое решение, реализуемое в пилотном проекте в Южной операционной зоне, полностью удовлетворяет всем государственным стандартам.

**Серверные компоненты**

Для работы рассматриваемого комплекса используется следующий перечень программного обеспечения:

- операционная система — AstraLinuxSpecialEdition 1.7;
- база данных — Postgresql-11;
- веб-сервер — Apache2;
- для работы aplicationprograminterface — библиотеки .NET (используется сервис dotnet).

При проектировании комплекса принято решение свести к минимуму использование зарубежных программных, аппаратных компонентов. В качестве хостовой операционной системы использованаAstraLinux, дистрибутив SpecialEdition версии 1.7, релиз «Смоленск». Он предполагает максимальный уровень защищенности. Выбор в пользу дистрибутива был сделан в результате сравнения с другим подходящим аналогом – «Воронеж». Разработчиком обеих версий ОС является отечественная компания ООО «РусБИТтех-Астра».

**Табл. 1.** Сравнительный анализ дистрибутивов «Воронеж» и «Смоленск»

| Уровень защищенности | «Воронеж» (усиленный) | «Смоленск» (максимальный) |
|---|---|---|
| Мандатный контроль | + | + |
| Ролевое управление | + | + |
| Управление доступом (дискретное) | + | + |
| Управление доступом (мандатное) | - | + |
| Защита СУБД | + | + |
| «Киосок» - перечень разрешенных приложений | + | + |
| Работа с ЭЦП | + | + |
| Изоляция Docker | + | + |
| Замкнутая программная среда | + | + |

При разработке программного обеспечения проведен сравнительный анализ двух адаптивных СУБД, работающих на Linux: MySQL и PostgreSQL. Выбор был сделан в пользу второй по следующему ряду причин:

- полностью открытый исходный код;
- широкий функционал, возможность адаптировать под любые задачи;
- поддерживаются 160 из 179 обязательных пунктов ключевых принципов SQL;
- встроен паттерн проектирования MVCC;
- широкий выбор способов репликации.

Основной причиной выбора Postgres стала поддержка SSL. Что дает возможность сделать обмен данными между серверами группы горячего резервирования полностью безопасным. Передаваемые данные в обязательном порядке шифруются. Причем как между серверами, так и между клиентом и сервером. При тестировании скорости работы Postgres выявлено, что скорость работы ниже, чем у MySQL. Причина кроется в потреблении оперативной памяти: каждое клиентское подключение потребляет 10 Мб.

При проектировании программного обеспечения не смогли найти аналог для библиотек apiMicrosoftdotnet. В дальнейшем планируется миграция на альтернативные библиотеки собственной разработки либо аналоги от сторонних разработчиков. При интеграции был использован ASP.NET CoreRuntime. В качестве программного средства для работы с электронными ключами (открытая, закрытая форма) для шифрования трафика применяется СКЗИ «КриптоПро CSP» [3].

**Аппаратное обеспечение системы защищенного дистанционного управления**

Для эксплуатации предполагается использование следующих аппаратных ресурсов:

- сервер VegmanYadroYadro R120 (2 шт.);
- биометрический датчик ZKTeco (4 шт.);
- коммутаторы Eltex MES2324 (2 шт.);
- межсетевые экраны Usergate D200F (2 шт.).

При выборе сетевого, серверного оборудования упор сделан на отечественного производителя. Основная причина — государственная корпорация АО «СО ЕЭС» взяла курс на импортозамещение. В проекте изначально планировалось использовать межсетевые экраны ASA 5515, коммутаторы Cisco 2960, сервера Lenovo. Последние события привели к невозможности эксплуатации перечисленного оборудования по причинам, связанным с информационной безопасностью и отсутствием технической поддержки [1].

Перечисленное выше оборудование по внутренним каналам связи выполняет коммутацию с доменом СК-11, серверами СК11.Proxy, расположенными в демилитаризованной зоне (продукт компании АО «Монитор Электрик»).

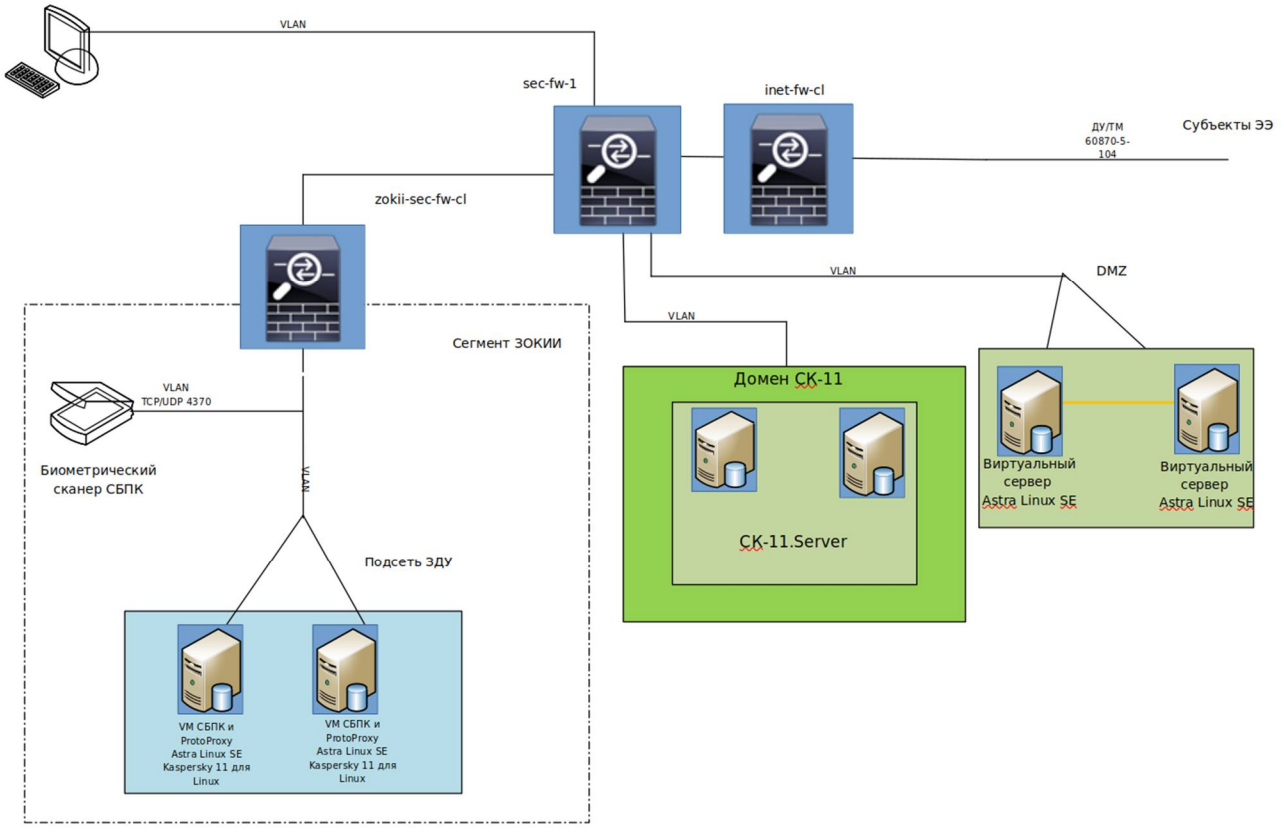


**Рис. 1.** Структурная схема программно-аппаратного комплекса защищенного дистанционного управления

Сервера, используемые для установки СБПК, имеют следующие технические характеристики:

- оперативная память — 32 Гб;
- количество ядер центрального процессора — 12;
- частота ЦП — 3.2 ГГц;
- объем хранилища — 1 Тб.

Защита информации от несанкционированного доступа реализована путем обмена данными с использованием защищенных каналов связи в одном VLAN. В качестве транспортного протокола используется HTTPS. Для шифрования применяется ключ электронной подписи, сертификат выпущенный собственным удостоверяющим центром АО «СО ЕЭС». Администрирование серверов выполняется с использованием протокола SSH v2 [1]. Также информационная безопасность обеспечивается за счет использования антивирусной защиты Kaspersky 11 for Linux.

**Программное обеспечение системы защищенного дистанционного управления**

При подтверждении разовых команд дистанционного управления с использованием данных биометрии и предварительно согласованных приложений используется разработанная АО «Монитор Электрик» программа для ЭВМ «NT_104.ProtoProxy». Программное обеспечение осуществляет поддержку адаптера интерфейса сервиса биометрического подтверждения. NT_104 [6]. ProtoProxy гарантирует формирование, передачу команд ДУ по протоколу МЭК 60870-5-104 только при подтверждении операции

со стороны СБПК. Это предполагает формирование кадра МЭК 60870-5-104 только при положительном биометрическом подтверждении [8].

В модели СК-11 для автоматизированного рабочего места (АРМ) диспетчера сопоставляется Биометрический сканер СБПК. Он имеет уникальный идентификатор. В дополнительных полях телеуправления будут передаваться следующие параметры:

- идентификатор биометрического сканера СБПК;
- идентификатор команды ДУ;
- идентификатор программы переключений ДУ.

Адаптер интерфейса системы биометрической проверки команд обеспечивает встраивание в NT_104.ProtoProxy функций взаимодействия с СБПК. Функции безопасности для взаимодействия с сервером биометрической обработки будут реализованы встроенными средствами ОС, наложенными средствами защиты информации. Запись информации о событиях биометрического подтверждения команд, программ переключений будет фиксироваться в журнале работы приложения.

Биометрический сканер СБПК, отмеченный на схеме (рис. 1), отвечает за подтверждение полномочий отправки команд дистанционного управления с коммуникационного процессора СК11.Proxy на субъекты электроэнергетики. Сам сканер не хранит в себе биометрические данные пользователей системы. Отправка команды о получении биометрических данных СБПК согласно составу диспетчеров, находящихся на смене [9].

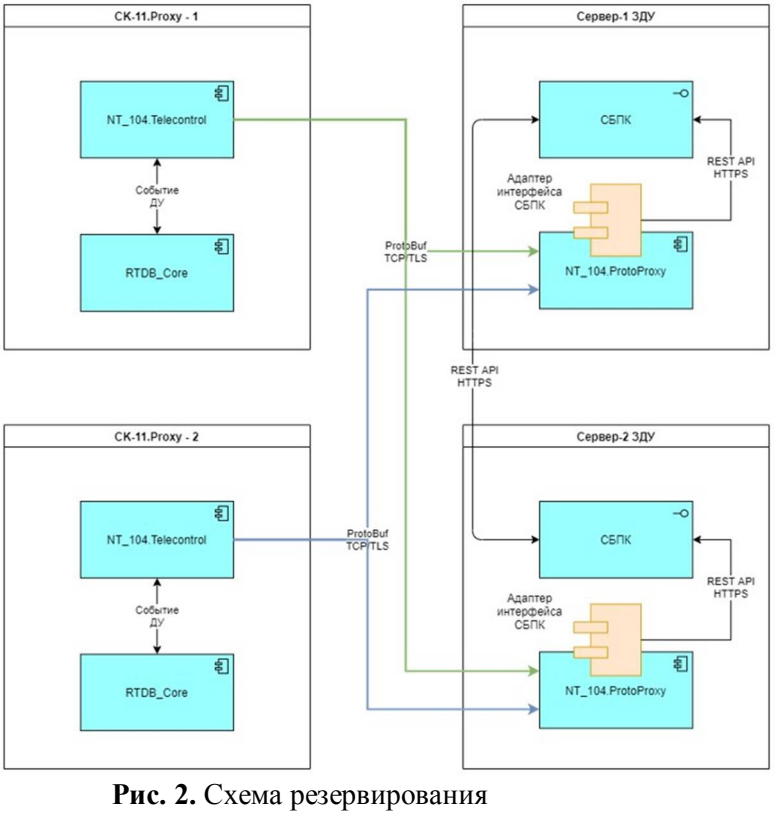


**Рис. 2.** Схема резервирования

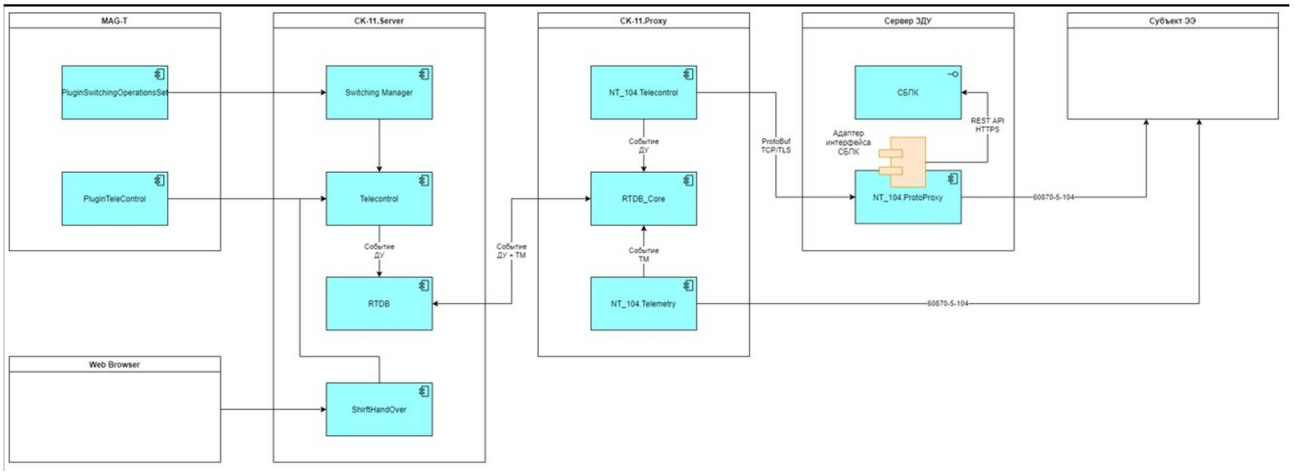


**Рис 3.** Схема информационных потоков

Схема работы структурного обмена работает согласно следующим правилам:

- отправка команд дистанционного управления возможна только в случае регистрации сотрудника на смене;
- возможна отправка команд единичных, а также непосредственно из программ переключений;
- сервис обработки дистанционного управления отправляет событие дистанционного управления (ДУ) в БДРВ коммуникационного процессора СК11.Proxy — используется механизм синхронизации;
- событие ДУ из БДРВ СК11.Proxy отправляют в NT_104.Telecontrol (если функционал возложен на сервер СК-11 SCADA, то работа будет выполнена сервисом БДРВ СК-11);
- NT_104.Telecontrol выполняет отправку событий в NT_104.ProtoProxy;
- NT_104.ProtoProxy отправляет запрос в службу биометрической авторизации, и при положительном ответе команда будет отправлена на объект электроэнергетики (при отрицательном ответе возвращается код ошибки) [20].

Программно-аппаратный комплекс соответствует всем требованиям, предъявляемым к защищенным объектам критической информационной инфраструктуры. Сервис NT_104.ProtoProxy устанавливает соединение при отправке первой команды ДУ. Разрыв соединения происходит по таймауту. Телеметрия передается через NT_104.Telemetry, транспортная сессия постоянна. До истечения таймаута все команды, отправленные с рабочего места диспетчера, не требуют повторной авторизации [11].

Прием и передача смены выполняются средствами дополнительного модуля, разработанного подрядной организацией. Используются плагины ShiftHandover.MFADataPlugin, ShiftHandover.MFAPlugin. Описание перечисленных выше модулей представлено на рис. 4.

```
<?xml version="1.0" encoding="utf-8" ?>
<Plugins>
  <Plugin FileName="Monitel.ShiftHandover.DispJournalPlugin.dll" />
  <Plugin FileName="Monitel.ShiftHandover.ReportPlugin.dll" />
  <Plugin FileName="Monitel.ShiftHandover.DJVisasPlugin.dll" />
  <Plugin FileName="Monitel.ShiftHandover.DirectivesPlugin.dll" />
  <Plugin FileName="Monitel.ShiftHandover.MFADataPlugin.dll" />
  <Plugin FileName="Monitel.ShiftHandover.MFAPlugin.dll" />
</Plugins>
```

**Рис. 4.** Пример описания плагина в формате .xml

**Сравнительный анализ скорости чтения/записи баз данных MySQL и PostgreSQL**

Одним из критериев скорости работы серверов защищенного дистанционного управления является чтение/запись в базу данных. В процессе проектирования было проведено тестирование с помощью тестов, разработанных автором Дмитрием Кравчуком. Само тестирование было выполнено на серверном оборудовании с характеристиками, приведенными выше (производитель — VegmanYadro). Причина использования оборудования этого производителя: вендор позиционирует себя как отечественный. Компания АО «СО ЕЭС» имеет право закупать и использовать лишь продукцию, произведенную на территории Российской Федерации [19].

Для работы были использованы тесты pgbench. Но для их написания применен синтаксис SysBenchLua. В дальнейшем полученный инструментарий был задействован для тестирования на сравниваемых базах данных — MySQL и Postgres [5]. Основной целью создания данных тестов является высокая нагрузка на базу данных. Для решения поставленной задачи соблюдено несколько условий:

– запуск SysBench должен выполняться с параметром percentile и max-requests, равным нулю;
– улучшение параллелизма достигается за счет использования ветви concurrency_kit.

Для примера на графике выполненных тестов под нагрузкой отображены ещё два сервера: MySQLOracle и MySQLPercona. Для сравнения были выполнены тесты Point SELECT, OLTP RO, OLTP RW [12].

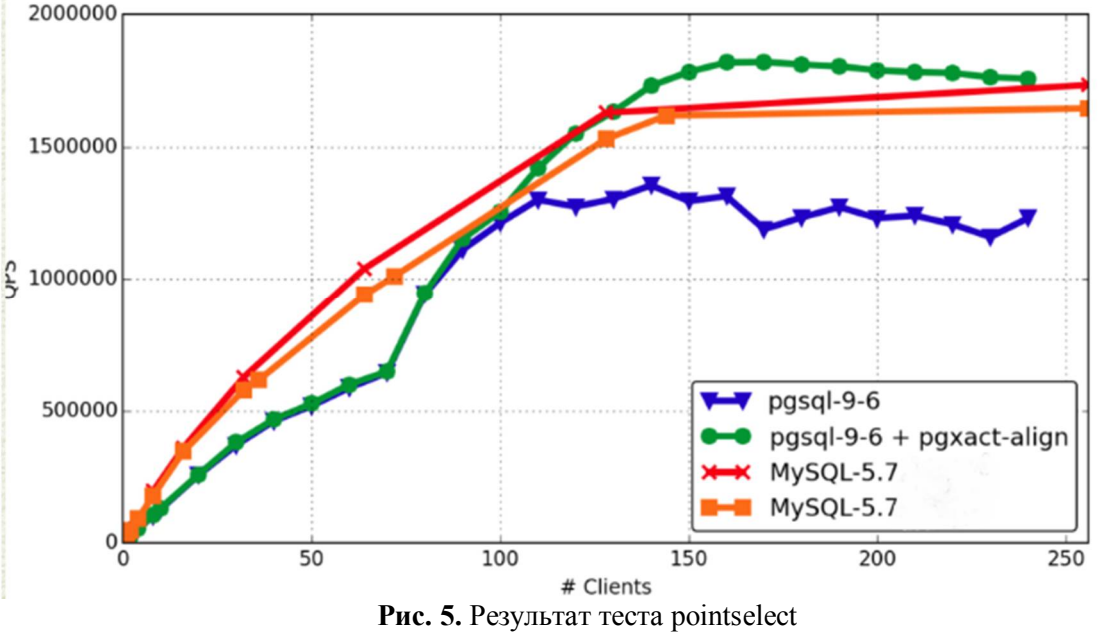


**Рис. 5.** Результат теста pointselect

На рис. 5 представлены 4 графика, отображающие производительность в разных условиях. Ось абсцисс обозначает количество клиентов, подключившихся за единицу времени. Ось ординат, обозначенная как QPS, отображает потребность в ресурсах и указывает на объем обработанного поискового трафика. На рис. 6 отображены графики тестирования нагрузки на базу данных postgresql версии 9.6 и MySQL 5.7.

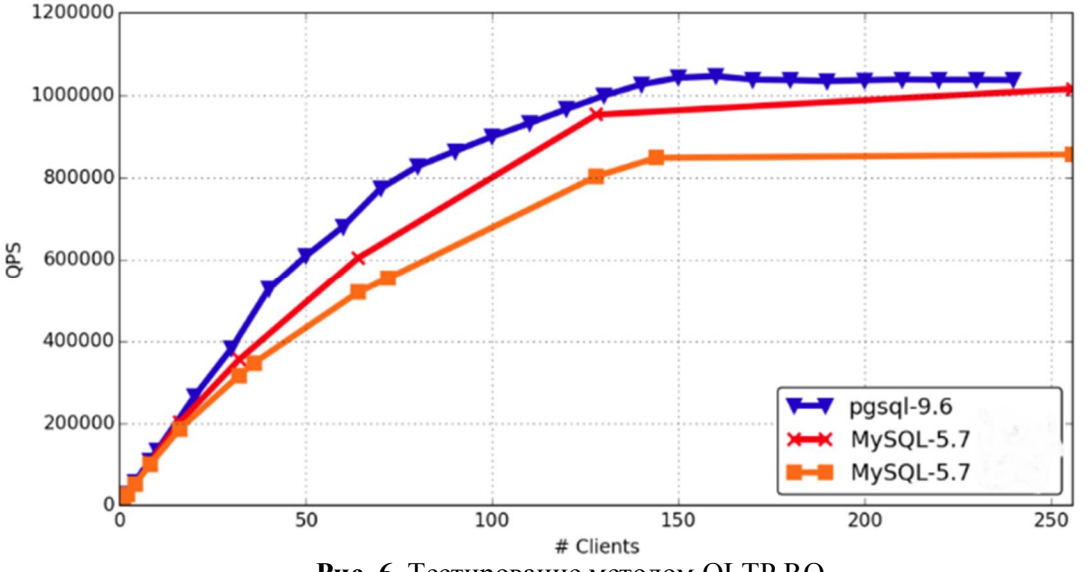


**Рис. 6.** Тестирование методом OLTP RO

На основании проведенных выше тестов можно сделать вывод о более высокой производительности базы данных PostgreSQL, что делает её использование предпочтительнее [5].

**Защита передаваемых вне защищенной сети данных**

Для решения задачи, связанной с передачей команд дистанционного управления, требуется уровень защищенности, рекомендованный Федеральной службой по техническому и экспортному контролю. В качестве межсетевых экранов, предотвращающих вторжение злоумышленников, использован кластер Usergate D200F. В качестве конкурента изначально выступал Cisco ASA 5515. Выбор был сделан в пользу Usergate D200F по трем причинам: большая производительность, широкий функционал и отечественное производство. Разработка проекта была начата задолго до сложностей с поставками сетевого оборудования из-за рубежа [13].

Предварительно было выполнено сравнение оборудования. Самым важным преимуществом Usergate D200F является наличие функционала, которого нет у Cisco ASA. Категория межсетевых экранов Next-GenerationFirewall (NGFW), к которой относится модель D200F, дополнена такими опциями:

- СОВ — система обнаружения вторжений;
- возможность выбора режима функционирования — прокси-сервер, межсетевой экран, реверс-прокси, комбинированные режимы работы;
- возможность централизованного управления.

Ключевыми отличиями, определившими использование именно NGWF, стали наличие возможности централизованного управления и производительность [18]. Основные характеристики Usergate D200F:

- пропускная способность межсетевого экрана (МСЭ) — до 18 Гб/с;
- производительность межсетевого экрана, трафик emix — до 18 Гб/с;
- количество одновременно запущенных TCP-сессий — до 8 млн.;
- новых сессий в секунду, шт. — до 50 000;
- производительность системы обнаружения вторжений, трафик emix — до 1,8 Гб/с;
- фильтрация контента, Гб/с — до 8,7 Гб/с.

Производительность обеспечена аппаратной платформой. Данная модель оборудована процессором с 4 физическими ядрами и оперативной памятью DDR4 16 Гб. Сам межсетевой экран представляет собой полноценный Linux-сервер с разработанной специалистами ООО «Usergate» операционной системой. Cisco 5515 имеет менее впечатляющие характеристики. Количество оперативной памяти составляет всего 8 Гб, причем пропускная способность при динамической проверке пакетов ниже более, чем в 10 раз (всего 1,2 Гб/с) [14].

**Применяемый в техническом решении протокол**

Для транспорта данных используется утвержденный на государственном уровне протокол телемеханики МЭК 104. Основные положения касательно использования отражены в документе «О приведении систем телемеханики и связи на генерирующих предприятиях электроэнергетики, входящих в состав холдинга ОАО РАО «ЕЭС России», в соответствие с требованиями балансирующего рынка» (Приказ №603 от 09.09.05 г. ОАО РАО «ЕЭС России»). Его действие распространяется на все энергетические компании [17].

Характеристики аппаратной и программной части проекта полностью вписываются в рамки требований, обозначенных в Приказе №603. К таковым относятся:

- наличие одной основной и одной резервной линии связи (минимальная пропускная способность – 64 кБит/с);
- лимиты времени на передачу оперативной информации;
- организация прямых каналов связи до объектов управления от ИА, ОДУ, РДУ.

В процессе интеграции проекта возникли проблемы, связанные со спорными моментами, такими как метка времени, отсутствие часовых поясов, возможность расширения. Причем в зарубежных протоколах данные противоречия отсутствуют. Например, метка времени в формате UTC в зарубежном аналоге есть, а в протоколе отечественной разработки отсутствует. Проблема в рамках защищенного дистанционного управления была решена за счет использования протокола NTP (используется стандартная клиент-серверная модель). В качестве источников времени выступают контроллеры домена WindowsServer [15].

Протокол IEC 60870-5-5 также не предполагает наличия часовых поясов в своих кадрах. Но наличие в метке 7 свободных байт позволяет задать текущий часовой пояс при необходимости. Точность времени является критичной для получения/передачи телеметрии, отправки команд по защищенному дистанционному каналу в АО «СО ЕЭС». Прикладное программное обеспечение снабжено функцией, прописывающей метку часового пояса в свободные байты кадра [7].

Протокол имеет потенциал для дальнейшего развития. Причина кроется в изначально заложенной возможности расширения. В современной редакции реально используется приблизительно 20% заложенных в него кадров. Этот «буфер» позволит в дальнейшем существенно расширить перечень передаваемой телеинформации [2].

**Типовая схема организации и подключения сегмента защищенного дистанционного управления на физическом и канальном уровне**

Для работы системы защищенного дистанционного управления создана отдельная подсеть со своим перечнем VLAN. Проектирование данного сегмента выполнялось с учетом требований, предъявляемых к надежности. Например, трафик должен шифроваться, а потому в качестве средства защиты данных использован криптографический шлюз S-terraG-1000 КС2. Максимальная производительность шифрования находится на одном уровне с NGFWUsergateD200F, используемыми в качестве межсетевых экранов и выполняющими функцию защиты трафика. Шифрование трафика соответствует требованиям, предъявляемым к защищенным объектам критической информационной инфраструктуры

(ЗОКИИ). S-terraG-1000 КС2 поддерживает ГОСТ Р 34.13-2015, что является одним из основных требований, предъявляемых к ЗОКИИ, проектируемых и работающих в государственных структурах [6]. Выбранное оборудование прошло сертификацию ФСТЭК и входит в перечень криптографических шлюзов, разрешенных к использованию в сегментах ЗОКИИ [16].

Для решения задачи сетевого проектирования использованы 7 отдельных VLAN для логического построения сети. Схема физического и логического соединения представлена на рис. 7. Подключение выполняется к портам Ethernet с помощью витой пары категории 6 [4].

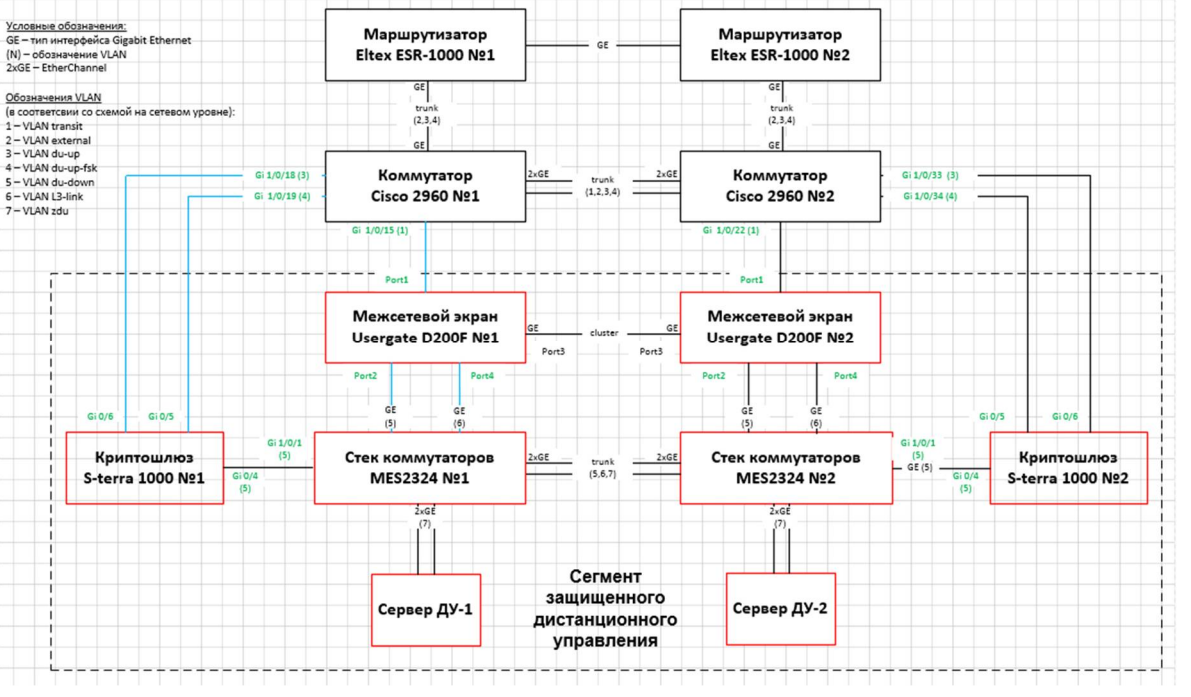


**Рис. 7.** Схема организации и подключения сегмента

## Заключение

В результате успешной реализации проекта были достигнуты все поставленные цели: выполнено проектирование информационно-управляющей системы, реализовано защищенное дистанционное управление. Стало возможным выполнение технологических работ в удаленном режиме. Отсутствует необходимость задействовать оперативный персонал на местах, что повышает эффективность работ. Ранее для выполнения аналогичных переключений требовалось более 3 часов. Внедрение защищенного дистанционно управления позволило снизить затраты времени в 6 раз.

## Литература

1. Олифер В. Компьютерные сети: принципы, технологии, протоколы. Санкт-Петербург: Питер, 2018. – 992 с.

2. *Будко П. А., Кулешов И. А., Курносов В. И., Мирошников В. И.* Инфокоммуникационные сети: энциклопедия. Кн. 4. Гетерогенные сети связи: принципы построения, методы синтеза, эффективность, цена, качество /под ред. проф. В. И. Мирошникова. – М.: Наука, 2020. – 683 с.

3. Родичев Ю. А. Нормативная база и стандарты в области информационной безопасности. Санкт-Петербург: Питер, 2018. – 256 с.

4. *Сычев К. И.* Многокритериальное проектирование мультисервисных сетей связи. СПб.: Изд-во Политехи, ун-та, 2018. - 272 с.

5. *Домбровская Г.Р.* Оптимизация запросов PostgreSQL. Москва: ДМК Пресс, 2022. – 278 с.

6. *Власенко А.В.* Событийное реагирование на инциденты информационной безопасности // Цифровая трансформация науки и образования. НАЛЬЧИК, 2021. С. 230-236.

7. *Виноградeнко А. М.* Методология интеллектуального контроля технического состояния автоматизированной системы связи специального назначения. СПб.: Наукоемкие технологии, 2020. 80с.

8. *Николаенко Е.П.* Управление инцидентами информационной безопасности // ЭМПИ: экономика, менеджмент, прикладная информатика. Брянск: Брянский государственный технический университет, 2019. С. 207-210.

9. *Porsev K. I., Sorokin A. V.* Management of Innovations and Knowledge in the Structure of the Enterprise Integrated Information Environment, In: Proceedings of the 2020 International Conference Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS), 2020. Pp. 283–285.

10. *Rihar L. Zuzek T., Berlec T., Kusar J.* Standard Risk Management Model for Infrastructure Projects //Risk Management in Construction Projects. IntechOpen. 2019. DOI: 10.5772/intechopen.83389.

11. *Budko P. A., Vinogradenko A. M., Mezhenov A. V., Zhuravlyova N. G.* Method of adaptive control of technical states of radioelectronic systems // Advances in Signal Processing. Theories, Algorithms, and System Control. Intelligens Systems Reference Library. Springer-Verlag 2020. Vol. 184. Chapter 11. Pp. 137-151.

12. *Виноградeнко А. М., Будко Н. П.* Адаптивный контроль технического состояния сложных технических объектов на основе интеллектуальных технологий // T-Comm: Телекоммуникации и транспорт. 2020. Т. 14. № 1. С. 25–35. DOI: 10.36724/2072-8735-2020-14-1-25-35.

13. *Turskis Z., Goranin N., Nurusheva A., Boranbayev S.* Information Security Risk Assessment in Critical Infrastructure: A Hybrid MCDM Approach // Informatica. 2019. Vol. 30(1). Pp. 187–211. DOI:10.15388/Informatica.2019.203.

14. *Денисова А.И.* Моделирование рисков разработки и реализации инфраструктурного проекта на основе методов сетевого планирования // Вестник университета. 2019. № 12. С. 56-65. DOI: 10.26425/1816-4277-2019-12-56-65.

15. *Кузьмина Н. А.* Системы фиксации и распознавания несанкционированного проникновения в охраняемую зону как элемент эффективной безопасности объекта транспортной инфраструктуры //T-Comm: Телекоммуникации и транспорт. 2018. Т. 12, № 5. С. 47-52. doi:10.24411/20728735201810086.

16. *Сухих С. Н., Николаев В. А., Кротов А. Ю.* О развитии технических средств охраны с применением Единого специализированного объектового протокола // Материалы международной научнотехнической конференции «Системы безопасности». Москва, 2020. С. 240-244.

17. *Климов А. В., Николаев В. А., Кротов А. Ю.* О создании технических средств охраны нового поколения, работающих с использованием Единого специализированного объектового протокола // Академический вестник войск национальной гвардии Российской Федерации. 2020. № 3. С. 40-43.

18. *Свиридов В. В.* Применение робототехнических комплексов охраны и обороны критически важных объектов Ракетных войск стратегического назначения // Военная мысль. 2021. № 6. С. 57-64.

19. *Исхаков А. Ю., Исхаков С.Ю.* Модели нормализации данных в системах управления событиями безопасности РТК. М.: Институт проблем управления им. В.А. Трапезникова РАН, 2020. С. 1390 – 1399.

20. *Крыжановский А.В.* Управление инцидентами информационной безопасности. Волгоград: Волгоградский государственный университет, 2019. С. 30-33.

# DESIGN OF A SECURE REMOTE CONTROL SYSTEM

**DMITRY A. LYUBIMENKO**
Chief Specialist of the Information Infrastructure Systems Service of "SO UPS" Volgograd, Russia,
lubimenko-d@bk.ru

**ABSTRACT**

**Introduction**: Integration into the system of monitoring, management of energy subjects of the protected remote control (ZDU) implemented using the biometric command recognition system (SBPC). **Purpose**: Development and implementation of an information management system to control users with access to sending remote control commands from a communication processor to energy entities. **Results**: The information and control system allows you to generate information messages to dispatching personnel, perform switching by remote control. The complex was designed, tested, and put into commercial operation. A hot backup group of two Vegman Yadro servers has been deployed. Astra Linux Special Edition is used as the host operating system. Industrial servers, biometrics scanners, access switches are located in a secure subnet (allocated in a separate segment). Data protection, traffic encryption is performed using the domestic firewall of the new generation Usergate D200 operating in cluster mode (active-passive). A system of identification and authentication of users in the system has been developed. The functionality of the remote control command transmission system has been tested. The hot backup group assumes the possibility of reducing reliability by 50% (failure of one of the servers is allowed). The main task, involving the introduction of a remote control system, is 100% completed. **Practical relevance**: The protected remote control system allows you to control users with the rights to send remote control commands from the CK11.Proxy communication processor developed by Monitor Electric JSC. The authorization tool for sending the command is a biometric fingerprint scanner. Data transport is implemented using the IEC 60870-5-104 protocol. Logging of all events that have arisen in the system — arising as a result of user authorization confirmations - has been implemented. Data about execution, cancellation, and confirmation of commands are saved.

**Keywords:** control; remote; system; command; protected.

**REFERENCES**

1. Olifer V. Computer networks: principles, technologies, protocols. St. Petersburg: Peter, 2018. – 992 p.

2. Budko P. A., Kuleshov I. A., Kurnosov V. I., Miroshnikov V. I. Infocommunication networks: encyclopedia. Book 4. Heterogeneous communication networks: principles of construction, synthesis methods, efficiency, price, quality / edited by prof. V. I. Miroshnikov. – M.: Nauka, 2020. – 683 p. (In Rus)

3. Rodichev Yu. A. Regulatory framework and standards in the regional information security system. St. Petersburg: Peter, 2018. – 256 p. (In Rus)

4. Sychev K. I. Multicriteria design of multiservice communication networks. St. Petersburg: Publishing House of the Polytechnic University, 2018. - 272 p. (In Rus)

5. Dombrovskaya G.R. Optimization of PostgreSQL queries. Moscow: DMK Press, 2022. – 278 p. (In Rus)

6. Vlasenko A.V. Event response to information security incidents // Digital transformation of science and education. NALCHIK, 2021. pp. 230-236. (In Rus)

7. Vinogradenko A.M. Methodology of intellectual control of the technical condition of the automated communication system of special purpose. SPb.:Science-intensive technologies, 2020. 80s. (In Rus)

8. Nikolaenko E.P. Information security incident management // EMPI: economics, management, applied informatics. Bryansk: Bryansk State Technical University, 2019. pp. 207-210. (In Rus)

9. Porsev K. I., Sorokin A. V. Management of Innovations and Knowledge in the Structure of the Enterprise Integrated Information Environment, In: Proceedings of the 2020 International Conference Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS), 2020. Pp. 283–285. (In Rus)

10. Rihar L. Zuzek T., Berlec T., Kusar J. Standard Risk Management Model for Infrastructure Projects //Risk Management in Construction Projects. IntechOpen. 2019. DOI: 10.5772/intechopen.83389.

11. Budko P. A., Vinogradenko A. M., Mezhenov A. V., Zhuravlyova N. G. Method of adaptive control of technical states of radioelectronic systems // Advances in Signal Processing. Theories, Algorithms, and System Control. Intelligens Systems Reference Library. Springer-Verlag 2020. Vol. 184. Chapter 11. Pp. 137-151. (In Rus)

12. Vinogradenko A.M., Budko N. P. Adaptive control of the technical condition of complex technical objects based on intelligent technologies // T-Comm: Telecommunications and Transport. 2020. Vol. 14. No. 1. pp. 25-35. DOI: 10.36724/2072-8735-2020-14-1-25-35. (In Rus)

13. Turskis Z., Goranin N., Nurusheva A., Boranbayev S. Information Security Risk Assessment in Critical Infrastructure: A Hybrid MCDM Approach // Informatica. 2019. Vol. 30(1). Pp. 187–211. DOI:10.15388/Informatica.2019.203.

14. Denisova A.I. Risk modeling of the development and implementation of an infrastructure project based on network planning methods // Bulletin of the University. 2019. No. 12. pp. 56-65. DOI: 10.26425/1816-4277-2019-12-56-65. (In Rus)

15. Kuzmina N. A. Systems for fixing and recognizing unauthorized entry into a protected area as an element of effective security of a transport infrastructure facility //T-Comm: Telecommunications and Transport. 2018. Vol. 12, No. 5. pp. 47-52. doi:10.24411/20728735201810086. (In Rus)

16. Sukhoi S. N., Nikolaev V. A., Krotov A. Yu. On the development of technical means of protection using a single specialized object protocol // Materials of the international scientific and technical conference "Security systems". Moscow, 2020. pp. 240-244. (In Rus)

17. Klimov A.V., Nikolaev V. A., Krotov A. Yu. On the creation of new generation security equipment operating using a single specialized object protocol // Academic Bulletin of the National Guard Troops of the Russian Federation. 2020. No. 3. pp. 40-43. (In Rus)

18. Sviridov V. V. Application of robotic complexes for the protection and defense of critical objects of Strategic Missile forces // Military thought. 2021. No. 6. pp. 57-64. (In Rus)

19. Iskhakov A. Yu., Iskhakov S.Yu. Data normalization models in RTK security event management systems. Moscow: V.A. Trapeznikov Institute of Management Problems of the Russian Academy of Sciences, 2020. pp. 1390 – 1399. (In Rus)

20. Kryzhanovsky A.V. Information security incident management. Volgograd: Volgograd State University, 2019. pp. 30-33. (In Rus)